VERTRAG

Über die Verarbeitung von personenbezogenen Daten im Sinne des Art. 28 Abs. 3 der Europäischen Datenschutz Grundverordnung 2016/679 („DSGVO“)

zwischen	Ihrem Unternehmen
	nachfolgend Auftraggeber (Verantwortlicher) genannt
und	Göbel+Lenze Direktmarketing GmbH vertreten durch Wulf Henrichs Stahlgruberring 22 81829 München
	nachfolgend Auftragnehmer (Auftragsverarbeiter) genannt.

Göbel+Lenze
Direktmarketing GmbH
Stahlgruberring 22
81829 München

Fon (089) 42 71 88 – 840
fax (089) 42 71 88 – 878
web www.goebel-lenze.de

Deutsche Bank AG
IBAN:
DE65700700240228806600
BIC/SWIFT-CODE:
DEUTDEDBMUC

Geschäftsführer
Wulf Henrichs

Registergericht München HRB 69 740

Finanzamt München
USt.-Id-Nr. DE 129 314 019
Steuernummer 812/45460

Präambel

Dieser Vertrag konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich bei der Erbringung der beauftragten Dienstleistung ergeben. Er findet Anwendung auf alle Tätigkeiten, die mit der beauftragten Dienstleistung in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer beauftragte weitere Auftragsverarbeiter auftragsgegenständliche personenbezogene Daten („Daten“) im Auftrag des Auftraggebers im Sinne der Art. 4 Nr. 2 und 28 DSGVO verarbeiten („Auftragsverarbeitung“).

1. Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

1.1. Gegenstand, Dauer, Art und Zweck der Auftragsverarbeitung sowie die Art der Daten und die Kategorien betroffener Personen sind in Nr. I der Anlage 1 zu diesem Vertrag aufgenommen. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen bedürfen eines dokumentierten elektronischen Formats.

1.2. Die in diesem Vertrag vereinbarten Dienstleistungen werden ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung von Dienstleistungen oder von Teilarbeiten dazu in ein Drittland („Verlagerung“) bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Europäischen Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln). Alle zu Beginn der Verarbeitung auf Basis dieser Grundsätze bereits vorgenommenen Verlagerungen sind in Nr. II der Anlage 1 zu diesem Vertrag aufgenommen.

1.3. Der Vertrag tritt mit Bestätigung dieser Vereinbarung in Kraft und gilt für die Dauer der Beauftragung. Dieser kann von beiden Parteien schriftlich mit einer Frist von 3 Monaten zum Quartalsende gekündigt werden, sofern sich aus den Bestimmungen dieses Vertrages nichts anderes ergibt. Der Auftraggeber kann diesen Vertrag jederzeit ohne Einhaltung einer Frist kündigen, (1) wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, oder (2) der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will, oder (3) der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar. Die Kündigung hat schriftlich oder in einem dokumentierten elektronischen Format zu erfolgen (Sonderkündigungsrecht bei schweren Datenschutzverstößen).

2. Rechte und Pflichten des Auftragnehmers

2.1. Der Auftragnehmer verarbeitet Daten von betroffenen Personen ausschließlich im Rahmen der getroffenen Vereinbarungen und der dokumentierten Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z.B. Ermittlung von Strafverfolgungs- oder Staatsschutzbehörden). In einem solchen Fall teilt der Auftragsverarbeiter dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO).

2.2. Vorbehaltlich des Art. 28 Abs. 3 Satz 2 lit. a DSGVO informiert der Auftragnehmer den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. In diesem Fall darf der Auftragnehmer die Umsetzung der Weisung solange aussetzen, bis die Parteien eine einvernehmliche Lösung gefunden haben.

Göbel+Lenze
Direktmarketing GmbH
Stahlgruberring 22
81829 München

Fon (089) 42 71 88 – 840
fax (089) 42 71 88 – 878
web www.goebel-lenze.de

Deutsche Bank AG
IBAN:
DE65700700240228806600
BIC/SWIFT-CODE:
DEUTDEDBMUC

Geschäftsführer
Wulf Henrichs

Registergericht München HRB 69 740

Finanzamt München
USt.-Id-Nr. DE 129 314 019
Steuernummer 812/45460

2.3. Der Auftragnehmer verwendet die zur Verarbeitung überlassenen Daten für keine anderen und insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt.

2.4. Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der Daten die Vertraulichkeit zu wahren und insbesondere alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftraggebers vertraulich zu behandeln. Diese Verpflichtung besteht auch nach Abschluss der Verarbeitung bzw. nach Beendigung des Vertrages fort. Der Auftragnehmer sichert insoweit zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden. Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet; Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.

2.5. Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapital III der DSGVO genannten Rechte der betroffenen Person nachzukommen (Art. 28 Abs. 3 lit. e DSGVO).

2.6. Der Auftragnehmer unterstützt den Auftraggeber in angemessener Weise bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten, wie etwa der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten oder bei erforderlichen Datenschutz-Folgenabschätzungen des Auftraggebers (Art. 28 Abs. 3 Satz 2 lit. f DSGVO). Er hat die dazu erforderlichen Angaben jeweils unverzüglich an den Auftraggeber weiterzuleiten.

2.7. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich über Störungen, Verstöße und Verletzungen datenschutzrechtlicher Bestimmungen oder der Vereinbarungen dieses Vertrages durch bei ihm beschäftigte Personen oder von ihm beteiligte Dritte. Dies gilt bereits beim Verdacht einer entsprechenden Störung und insbesondere im Hinblick auf mögliche Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DSGVO. Der Auftragnehmer sichert insoweit zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DSGVO). Meldungen nach Art. 33 oder 34 DSGVO darf der Auftragnehmer für den Auftraggeber nur nach vorheriger Weisung selbst durchführen. Er wird jedoch in jedem Falle unverzüglich alle erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die betroffenen Personen treffen und sich hierzu mit dem Auftraggeber absprechen.

2.8. Der Auftragnehmer wird dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO für die Auftragsverarbeitung niedergelegten Pflichten zur Verfügung stellen und – grundsätzlich nach vorheriger Terminvereinbarung – Überprüfungen und Inspektionen, die vom Auftraggeber oder einem anderen, von diesem beauftragten Prüfer, durchgeführt werden, ermöglichen und zu ihnen beitragen (Art. 28 Abs. 3 Satz 2 lit. h DSGVO). Ergänzend hierzu gelten die Ziffern 3.3 und 6 dieses Vertrages.

2.9. Die Verarbeitung von Daten in Privatwohnungen (Tele- bzw. Heimarbeit von Beschäftigten des Auftragnehmers) ist nur nach vorheriger Zustimmung des Auftraggebers gestattet. Soweit die Daten in einer Privatwohnung verarbeitet werden, ist vorher der Zugang zur Wohnung des Beschäftigten für Kontrollzwecke des Arbeitgebers vertraglich sicher zu stellen. Die Maßnahmen nach Art. 32 DSGVO sind auch in diesem Fall sicherzustellen.

2.10. Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DSGVO bekannt sind und er die mit der Erbringung der Dienstleistung beschäftigten Personen vor Aufnahme der Verarbeitung mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut gemacht hat. Er verpflichtet sich, auch die für diesen Auftrag relevanten Geheimnisschutzregeln zu beachten, die dem Auftraggeber obliegen. Diese sind, sofern gegeben, in Nr. III der Anlage 1 zu diesem Vertrag aufgenommen.

Göbel+Lenze
Direktmarketing GmbH
Stahlgruberring 22
81829 München

Fon (089) 42 71 88 – 840
fax (089) 42 71 88 – 878
web www.goebel-lenze.de

Deutsche Bank AG
IBAN:
DE65700700240228806600
BIC/SWIFT-CODE:
DEUTDEDBMUC

Geschäftsführer
Wulf Henrichs

Registergericht München HRB 69 740

Finanzamt München
USt.-Id-Nr. DE 129 314 019
Steuernummer 812/45460

2.11. Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisungen zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der Daten befugten Personen vor der Verarbeitung zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DSGVO) und diese Vertraulichkeits- bzw. Verschwiegenheitspflicht auch nach Beendigung des mit der zur Verarbeitung der Daten befugten Person geschlossenen Vertrages bzw. der Auftragsverarbeitung fortbesteht.

2.12. Der Auftragnehmer nennt dem Auftraggeber einen Ansprechpartner für im Rahmen dieses Vertrages anfallende Datenschutzfragen und als konkreten Weisungsempfänger auf Seiten des Auftragnehmers. Dieser (und der konkrete Weisungsberechtigte des Auftraggebers) ist in Nr. IV der Anlage 1 zu diesem Vertrag zu nennen. Bei einem Wechsel oder einer längerfristigen Verhinderung einer der genannten Personen ist dem anderen Vertragspartner unverzüglich in Schriftform oder einem dokumentierten elektronischen Format ein Nachfolger bzw. Vertreter mitzuteilen. Weisungen sind für ihre Geltungsdauer und anschließend noch für drei weitere, volle Kalenderjahre aufzubewahren.

2.13. Der Auftragnehmer hat Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt.

2.14. Sofern die gesetzlichen Voraussetzungen vorliegen hat der Auftragnehmer eine(n) Beauftragte(n) für den Datenschutz zu bestellen. Näheres hierzu, insbesondere die Kontaktdaten der oder des ggf. bestellen Beauftragten für den Datenschutz, ist in Nr. V der Anlage 1 zu diesem Vertrag festgelegt. Jeder Wechsel in der Person der(s) Datenschutzbeauftragten sowie die Erfüllung der gesetzlichen Voraussetzungen und die daraus folgende Bestellung eines(s) Datenschutzbeauftragten ist dem Auftraggeber schriftlich oder in einem dokumentierten elektronischen Format mitzuteilen.

2.15. Nach der Beendigung der Auftragsverarbeitung sind sämtliche beim Auftragnehmer vorhandenen oder an Subunternehmen gelangte Daten, Datenträger, Unterlagen und sonstige Materialen sowie insbesondere alle Verarbeitungs- und Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers herauszugeben oder datenschutzgerecht zu löschen bzw. zu vernichten. Näheres hierzu ist in Nr. VI der Anlage 1 zu diesem Vertrag festgelegt.

3. Rechte und Pflichten des Auftraggebers

3.1. Für die Beurteilung der Rechtmäßigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO ist allein der Auftraggeber verantwortlich.

3.2. Der Auftraggeber ist berechtigt, sich vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag und dem Hauptvertrag festgelegten Verpflichtungen zu überzeugen (vgl. Ziffer 2.8).

3.3. Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von ihm beauftragten Prüfer erforderlich sein, werden diese grundsätzlich zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorankündigung von wenigstens 28 Tagen durchgeführt. Im Falle einer Schutzverletzung i.S.d. Art. 4 Nr. 12 DSGVO und bei schwerwiegenden Vertragsverstößen können Inspektionen auch mit kürzerer Ankündigungsfrist durchgeführt werden. Der Auftragnehmer darf diese von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch

Göbel+Lenze
Direktmarketing GmbH
Stahlgruberring 22
81829 München

Fon (089) 42 71 88 – 840
fax (089) 42 71 88 – 878
web www.goebel-lenze.de

Deutsche Bank AG
IBAN:
DE65700700240228806600
BIC/SWIFT-CODE:
DEUTDEDBMUC

Geschäftsführer
Wulf Henrichs

Registergericht München HRB 69 740

Finanzamt München
USt.-Id-Nr. DE 129 314 019
Steuernummer 812/45460

den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

3.4. Der Auftraggeber hat den Auftragnehmer unverzüglich zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

3.5. Der Auftraggeber nennt dem Auftragnehmer einen Ansprechpartner für im Rahmen dieses Vertrages anfallende Datenschutzfragen und als konkreten Weisungsberechtigten des Auftraggebers. Dieser (und der konkrete Weisungsempfänger auf Seiten des Auftragnehmers) ist in Nr. IV der Anlage 1 zu diesem Vertrag zu nennen. Bei einem Wechsel oder einer längerfristigen Verhinderung einer der genannten Personen ist dem anderen Vertragspartner unverzüglich in Schriftform oder einem dokumentierten elektronischen Format ein Nachfolger bzw. Vertreter mitzuteilen.

3.6. Weisungen werden anfänglich durch den Hauptvertrag bzw. diesen Vertrag festgelegt. Spätere Weisungen sind grundsätzlich schriftlich oder in einem dokumentierten elektronischen Format an die vom Auftragnehmer bezeichnete Stelle (vgl. Nr. IV der Anlage 1 zu diesem Vertrag) zu erteilen. Mündliche Weisungen sind für ihre Gültigkeit unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen. Weisungen sind für ihre Geltungsdauer und drei weitere Jahre, beginnend mit dem Ablauf des Kalenderjahres, in dem die Geltung der Weisung endet, aufzubewahren.

3.7. Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

4. Anfragen betroffener Personen

4.1. Im Falle der Inanspruchnahme einer der Parteien durch eine betroffene Person wegen etwaiger Ansprüche nach Art. 82 DSGVO sind der Auftragnehmer und der Auftraggeber verpflichtet sich gegenseitig bei der Abwehr des Anspruchs im Rahmen ihrer jeweiligen Möglichkeiten zu unterstützen.

4.2. Wendet sich eine betroffene Person mit einer Aufforderung zur Berichtigung, Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen bzw. den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiterleiten, sofern eine Zuordnung an den Auftraggeber auf Basis der Angaben der betroffenen Person möglich ist. Der Auftragnehmer ist nur nach vorheriger Zustimmung oder Weisung des Auftraggebers berechtigt, betroffenen Personen oder anderen Dritten Auskünfte über Daten, deren Verarbeitung oder das Auftragsverhältnis zu geben.

5. Technische und organisatorische Maßnahmen

5.1. Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Der Auftragnehmer wird alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz-Grundverordnung, insbesondere deren Art. 32 DSGVO genügen. Diese technischen und organisatorischen Maßnahmen („TOM“) sind diesem Vertrag als Anlage 2 beigefügt. Sie beinhalten eine detaillierte Darstellung aller zum ermittelten Risiko passenden und unter Berücksichtigung der Schutzziele und der eingesetzten IT-Systeme und Verarbeitungsprozesse beim Auftragnehmer implementierten Maßnahmen. Der Auftragnehmer hat dabei insbesondere solche Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und

Göbel+Lenze
Direktmarketing GmbH
Stahlgruberring 22
81829 München

Fon (089) 42 71 88 – 840
fax (089) 42 71 88 – 878
web www.goebel-lenze.de

Deutsche Bank AG
IBAN:
DE65700700240228806600
BIC/SWIFT-CODE:
DEUTDEDBMUC

Geschäftsführer
Wulf Henrichs

Registergericht München HRB 69 740

Finanzamt München
USt.-Id-Nr. DE 129 314 019
Steuernummer 812/45460

Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen.

5.2. Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb. Die Maßnahmen beim Auftragnehmer oder einem beauftragten Subunternehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten sowie gesetzlich vorgesehenen Standards nicht unterschreiten. Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind zwischen Auftragnehmer und Auftraggeber abzustimmen. Wesentliche Änderungen der technischen und organisatorischen Maßnahmen muss der Auftragnehmer mit dem Auftraggeber schriftlich oder in einem dokumentierten elektronischen Format abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages und für drei weitere Jahre, beginnend mit dem Ende des Kalenderjahres, in dem dieser Vertrag endet, aufzubewahren.

5.3. Der Auftragnehmer sichert zu, seinen Pflichten nach Art. 32 Abs. 1 lit. d DSGVO nachzukommen und ein Verfahren zur regelmäßigen Überprüfung und Bewertung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen. Die Ergebnisse sind dem Auftraggeber jeweils mitzuteilen.

6. Garantien, Nachweise

6.1. Der Auftragnehmer garantiert, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit der Europäischen Datenschutz-Grundverordnung und diesem Vertrag erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet (Art. 28 Abs. 1 DSGVO). Er garantiert zudem, dass die durchgeführten technischen und organisatorischen Maßnahmen unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos ein angemessenes Schutzniveau gewährleisten (Art. 32 Abs. 1 DSGVO). Die Einhaltung dieser Garantien weist der Auftragnehmer dem Auftraggeber mit geeigneten Mitteln (z.B. Dokumente, Zertifikate, Audits, Testate etc.) nach. Näheres hierzu ist in Nr. VII der Anlage 1 zu diesem Vertrag festgelegt.

6.2. Sofern einschlägig verpflichtet sich der Auftragnehmer, den Auftraggeber über den vorläufigen oder endgültigen Ausschluss von genehmigten Verhaltensregeln nach Art. 41 Abs. 4 DSGVO und den Widerruf einer Zertifizierung nach Art. 42 Abs. 7 DSGVO unverzüglich zu informieren.

7. Subunternehmer (weitere Auftragsverarbeiter)

7.1. Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers bedarf grundsätzlich entweder der gesonderten Zustimmung des Auftraggebers im Einzelfall oder der allgemeinen Genehmigung (Art. 28 Abs. 2 DSGVO). Der Auftragnehmer muss in jedem Falle dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesem implementierten technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.

7.2. Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

7.3. Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der im Vertrag vereinbarten Leistung beauftragt. Nicht als Subunternehmerverhältnis im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur

Göbel+Lenze
Direktmarketing GmbH
Stahlgruberring 22
81829 München

Fon (089) 42 71 88 – 840
fax (089) 42 71 88 – 878
web www.goebel-lenze.de

Deutsche Bank AG
IBAN:
DE65700700240228806600
BIC/SWIFT-CODE:
DEUTDEDBMUC

Geschäftsführer
Wulf Henrichs

Registergericht München HRB 69 740

Finanzamt München
USt.-Id-Nr. DE 129 314 019
Steuernummer 812/45460

Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Hierzu zählen z.B. Telekommunikationsleistungen, Wartung und Benutzerservice (wenn kein Zugriff auf Daten des Auftraggebers erfolgen kann), Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Die Einbindung von Entsorgungsunternehmen ist jedoch anzeigepflichtig, wenn der Kern der Beauftragung die Entsorgung von Dokumenten/Datenträgern welche Daten des Auftraggebers enthalten, beinhaltet. Der Auftragnehmer wird jedoch auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen treffen und erforderliche Kontrollmaßnahmen ergreifen, um den Schutz und die Sicherheit der Daten des Auftraggebers zu gewährleisten.

7.4. Bei Beauftragung von Subunternehmern hat der Auftragnehmer vertraglich sicherzustellen, dass die zwischen ihm und dem Auftraggeber vereinbarten Regelungen auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

7.5. Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem dokumentierten elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DSGVO).

7.6. Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DSGVO bezüglich seiner Beschäftigten erfüllt hat.

7.7. Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

7.8. Die Entscheidungen darüber, ob Subunternehmer eingeschaltet werden dürfen und ggf. die dann folgende Verfahrensweise bei der Beauftragung von Subunternehmern ist in Nr. IX der Anlage 1 zu diesem Vertrag geregelt.

7.9. Gegebenenfalls abweichend von den Festlegungen in Nr. IX der Anlage 1 zu diesem Vertrag sind für den Auftragnehmer bereits bei Abschluss dieses Vertrages die in Nr. VIII der Anlage 1 zu diesem Vertrag bezeichneten Subunternehmer mit der Verarbeitung von Daten in dem dort genannten Umfang beschäftigt. Insoweit sichert der Auftragnehmer zu, dass die in dieser Ziffer 7 genannten Voraussetzungen für die Beauftragung dieser Subunternehmer eingehalten worden sind. Vorbehaltlich der Vorlage der Prüfunterlagen gemäß Ziffer 5 dieses Vertrages, erklärt sich der Auftraggeber mit der Beauftragung der in der Anlage genannten Subunternehmer einverstanden.

8. Haftung und Schadensersatz

8.1. Die Vertragsparteien haften entsprechend den einschlägigen gesetzlichen Bestimmungen, gegenüber betroffenen Personen insbesondere gemäß Art. 82 DSGVO.

8.2. Soweit der Auftraggeber wegen einer rechts- oder pflichtwidrigen Verarbeitung von Daten, die in den Verantwortungsbereich des Auftragnehmers oder eines von ihm beauftragten Dritten (Subunternehmer) fällt, in Anspruch genommen wird, stellt der Auftragnehmer den Auftraggeber von diesen Ansprüchen Dritter frei.

9. Schlussbestimmungen

9.1. Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen

Göbel+Lenze
Direktmarketing GmbH
Stahlgruberring 22
81829 München

Fon (089) 42 71 88 – 840
fax (089) 42 71 88 – 878
web www.goebel-lenze.de

Deutsche Bank AG
IBAN:
DE65700700240228806600
BIC/SWIFT-CODE:
DEUTDEDBMUC

Geschäftsführer
Wulf Henrichs

Registergericht München HRB
69 740

Finanzamt München
USt.-Id-Nr. DE 129 314 019
Steuernummer 812/45460

Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen und Beteiligten unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als „Verantwortlichem“ im Sinne der DSGVO liegen.

9.2. Die Einrede des Zurückbehaltungsrechts i.S.v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der dazugehörigen Datenträger ausgeschlossen.

9.3. Technische organisatorische Maßnahmen und jede Änderung zu diesen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmern) sind während der Laufzeit dieses Vertrages und für drei weitere Jahre, beginnend mit dem Ende des Kalenderjahres, in dem dieser Vertrag endet, aufzubewahren.

9.4. Mündliche Nebenabreden zu diesem Vertrag bzw. zu den mit diesem Vertrag geregelten Gegenständen wurden nicht getroffen. Gegebenenfalls bestehende, frühere mündliche Absprachen werden mit Zustandekommen dieses Vertrages aufgehoben.

9.5. Änderungen und Ergänzungen dieses Vertrages und aller seiner Bestandteile – einschließlich etwaiger Zusicherungen und Garantien des Auftraggebers – bedürfen einer schriftlichen Vereinbarung, die auch in einem dokumentierten elektronischen Format erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

9.6. Bei etwaigen Widersprüchen gehen Regelungen dieses Vertrages und seiner Anlagen den Regelungen des Hauptvertrages vor; die Anlagen dieses Vertrages gehen dem Vertrag vor.

9.7. Sollten einzelne Bestimmungen dieses Vertrages oder seiner Anlagen ganz oder teilweise unwirksam oder undurchführbar sein oder werden, so ist die Wirksamkeit der übrigen Regelungen hiervon nicht betroffen. In diesem Falle werden die Parteien einvernehmlich eine neue Regelung oder Ergänzung der bestehenden Regelung vereinbaren, die die unwirksame oder undurchführbare Regelung in einer Art und Weise ersetzt bzw. ergänzt, die der ursprünglich von den Parteien bei Abfassung dieses Vertrages und seiner Anlagen beabsichtigten Regelung am nächsten kommt, hätten sie denn die Unwirksamkeit oder Undurchführbarkeit bedacht. Dies gilt auch für Regelungslücken.

9.8. Dieser Vertrag und seine Anlagen unterliegen dem Recht der Bundesrepublik Deutschland.

Göbel+Lenze
Direktmarketing GmbH
Stahlgruberring 22
81829 München

Fon (089) 42 71 88 – 840
fax (089) 42 71 88 – 878
web www.goebel-lenze.de

Deutsche Bank AG
IBAN:
DE65700700240228806600
BIC/SWIFT-CODE:
DEUTDEDBMUC

Geschäftsführer
Wulf Henrichs

Registergericht München HRB
69 740

Finanzamt München
USt.-Id-Nr. DE 129 314 019
Steuernummer 812/45460

Anlage 1

zum VERTRAG ÜBER DIE VERARBEITUNG VON PERSONENBEZOGENEN DATEN IM SINNE DES ART. 28 ABS. 3 DER EUROPÄISCHEN DATENSCHUTZ-GRUNDVERORDNUNG 2016/679 (DSGVO)

***I. zu Ziffer 1.1** - Umfang, Art und Zweck der Auftragsverarbeitung, Art der personenbezogenen Daten und Kreis der betroffenen Personen*

Gegenstand des Auftrags:
Erbringung von Lettershop-Dienstleistungen

Umfang, Art und Zweck der Auftragsverarbeitung (beauftragte Leistungen):
-entsprechend der Definition von Art. 4 Nr. 2 DSGVO-
Die auftragsgegenständliche Verarbeitung besteht in der Datenübernahme und -aufbereitung für den Druck von personalisierten Werbemitteln sowie der Weiterverarbeitung durch Falzen, Zusammentragen und Kuvertieren.
Die personenbezogenen Daten werden der Göbel+Lenze Direktmarketing GmbH (Auftragnehmer) elektronisch von deren Kunden (Auftraggeber) zur Verfügung gestellt, auf den Systemen des Auftragnehmers (logisch getrennt von Daten anderer Auftraggeber) abgelegt und im Sinne des Auftragsgegenstands verarbeitet.
Vor Verwendung der Daten werden diese an einem nicht mit dem Unternehmensnetzwerk verbundenen Rechner auf mögliche Schadsoftware durch den IT-Verantwortlichen geprüft.

Ein Zugriff auf die Daten ist nur den zuständigen Beschäftigten des Auftragnehmers möglich. Die Zugriffsrechte sind im Rahmen des IT-Sicherheitskonzeptes geregelt. Nach Fertigstellung der Druckerzeugnisse erfolgt die abschließende Übergabe der fertig produzierten Werbe-/Informationssendungen an den ausgewählten Versender (z.B. Deutsche Post, DHL, Postcon, UPS).

Mit allen eingesetzten Unterauftragsverarbeitern bestehen die erforderlichen Verträge zur Auftragsverarbeitung.
Notwendige Ausdrucke der Daten werden – nachdem sie nicht mehr benötigt werden – über eine abgeschlossene Datentonne entsorgt. Mit dem für die Entsorgung beauftragten Unterauftragsverarbeiter besteht der erforderliche Vertrag zur Auftragsverarbeitung.

Elektronisch gespeicherte Daten werden entsprechend den Vorgaben im Vertrag mit dem Kunden vom Auftragnehmer gelöscht. Der Auftragnehmer wird jeweils direkt im Anschluss an einen erledigten Auftrag, spätestens nach 3 Monaten, die im Rahmen dieses Einzelauftrages verarbeiteten Daten datenschutzgerecht löschen bzw. vernichten oder vernichten lassen.

Göbel+Lenze
Direktmarketing GmbH
Stahlgruberring 22
81829 München

Fon (089) 42 71 88 – 840
fax (089) 42 71 88 – 878
web www.goebel-lenze.de

Deutsche Bank AG
IBAN:
DE65700700240228806600
BIC/SWIFT-CODE:
DEUTDEDBMUC

Geschäftsführer
Wulf Henrichs

Registergericht München HRB 69 740

Finanzamt München
USt.-Id-Nr. DE 129 314 019
Steuernummer 812/45460

Datenarten, die verarbeitet werden:

-entsprechend der Definition von Art. 4 Nr. 1, 9, 13, 14 und 15 DSGVO-

- ☒ Personenstammdaten (z.B. Anrede, Name, Vorname, Adresse, Titel, Funktion)
- ☒ Kommunikationsdaten (Telefon, E-Mail)
- ☐ Vertragsstammdaten (z.B. Vertragsbeziehungen, Produkt- und Vertragsinteresse)
- ☐ Kundenhistorie (z.B. Käufe, Angebote, Anfragen, Kaufverhalten)
- ☐ Vertragsstamm-, Vertragsabrechnungs- und Zahlungsdaten
- ☐ Planungs- und Steuerungsdaten
- ☐ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
- ☐ Technische Protokolldaten (z.B. Login, IP, Zeitstempel)
- ☐ Daten, die Nutzer in Nachrichten, Freitextfeldern oder als Inhalt von Dateien von sich aus übermitteln:

_____

☐ Besondere personenbezogene Daten gem. Art. 9 Abs. 1 DSGVO (rassische und ethnische Herkunft, politische Meinungen, religiöse und philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben, genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person):

_____

☐ Weitere Daten:

_____

Kreis der von der Datenverarbeitung betroffenen Personen:

-entsprechend der Definition von Art. 4 Nr. 1 DSGVO-

- ☒ Kunden des Auftraggebers
- ☐ Kunden von Kunden des Auftraggebers
- ☐ Beschäftigte des Auftraggebers
- ☐ Beschäftigte von Kunden des Auftraggebers
- ☐ Ansprechpartner von Lieferanten des Auftraggebers
- ☐ Ansprechpartner von Lieferanten von Kunden des Auftraggebers
- ☒ Interessenten des Auftraggebers
- ☐ Interessenten von Kunden des Auftraggebers
- ☐ Andere

_____

II. zu Ziffer 1.2 – *Bestehende Verlagerungen der vertraglich vereinbarten Dienstleistung (oder Teilen) in ein Drittland:*

Dienstleistung / Verarbeitungsprozess	Angabe zum Drittland	Bes. Vorr. der Artt. 44 ff. DSGVO
Keine		

Basisangaben - ERFORDERLICH

Drittstaat

Göbel+Lenze
Direktmarketing GmbH
Stahlgruberring 22
81829 München

Fon (089) 42 71 88 – 840
fax (089) 42 71 88 – 878
web www.goebel-lenze.de

Deutsche Bank AG
IBAN:
DE65700700240228806600
BIC/SWIFT-CODE:
DEUTDEDBMUC

Geschäftsführer
Wulf Henrichs

Registergericht München HRB 69 740

Finanzamt München
USt.-Id-Nr. DE 129 314 019
Steuernummer 812/45460

III. zu Ziffer 2.10 – *Für den Auftrag relevante Geheimnisschutzregeln:*

(z.B. Bank-, Fernmelde-, Sozial-, Berufsgeheimnisse nach § 203 StGB etc.)
keine

IV. zu Ziffer 2.12 und Ziffer 3.5 – *Weisungsbefugnis*

Weisungsberechtigte Personen des Auftraggebers sind:

- Geschäftsführung beim Auftraggeber
- Projektverantwortliche beim Auftraggeber

Weisungsempfänger beim Auftragnehmer sind:

- Wulf Henrichs, Geschäftsführer
- Mitarbeiter aus der Kundenberatung des Auftragnehmers

Für Weisung zu nutzende Kommunikationskanäle:

Telefon: +49 89 427188-840
E-Mail: info@goebel-lenze.de

V. zu Ziffer 2.14 – *Datenschutzbeauftragte(r)*

☒ Beim Auftragnehmer ist als Beauftragte(r) für den Datenschutz bestellt

Herr David Malzkorn
BAY-Q GmbH
Hultschiner Str. 8
81677 München
Telefon: + 49 (89) 90 420 49-0
E-Mail: datenschutz@goebel-lenze.de

VI. zu Ziffer 2.15 – *Löschpflichten*

☒ Der Auftragnehmer wird jeweils direkt im Anschluss an einen erledigten Auftrag, spätestens nach 3 Monaten, die im Rahmen dieses Einzelauftrages verarbeiteten Daten datenschutzgerecht löschen bzw. vernichten oder vernichten lassen.

Jede Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

Geheimnis

Weisung – ERFORDERLICH

DSB – ERFORDERLICH

Löschpflichten / ERFORDERLICH

Göbel+Lenze
Direktmarketing GmbH
Stahlgruberring 22
81829 München

Fon (089) 42 71 88 – 840
fax (089) 42 71 88 – 878
web www.goebel-lenze.de

Deutsche Bank AG
IBAN:
DE65700700240228806600
BIC/SWIFT-CODE:
DEUTDEDBMUC

Geschäftsführer
Wulf Henrichs

Registergericht München HRB 69 740

Finanzamt München
USt.-Id-Nr. DE 129 314 019
Steuernummer 812/45460

VII. zu Ziffer 6 – Nachweise

☒ Zertifikat zu Datenschutz- und / oder Informationssicherheit (ISO 27001)

Die Göbel+Lenze Direktmarketing GmbH ist nach der DIN EN ISO/IEC 27001:2017 als Full-Service Dienstleister für gedruckte Kundenkommunikation inkl. Lettershop und Fullfillment zertifiziert und befindet sich derzeit in der Vorbereitung einer Zertifizierung nach ISO 27701.

VIII. zu Ziffer 7.9 – Zu Beginn der Verarbeitung bereits beauftragte Subunternehmer:

Name und Adresse	Beschreibung der vom Subunternehr erbrachten Leistungen
Fa. Goserver GmbH Dachauer Str. 123, 80335 München	Wartung der DV-Anlage
Shred-it GmbH Klausnerring 1, 85551 Kirchheim	Akten- und Datenträgervernicht

IX. zu Ziffer 7 – Regelung zum Umgang mit Subunternehmern

☒ Der Auftraggeber genehmigt allgemein, dass der Auftragnehmer weitere bzw. andere Subunternehmer einbindet. Der Auftragnehmer hat den Auftraggeber aber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung eines Subunternehmers schriftlich oder in einem dokumentierten elektronischen Format zu informieren. Der Auftraggeber kann gegen derartige Änderungen Einspruch erheben. Liegt ein wichtiger datenschutzrechtlicher Grund für den Einspruch vor und die Parteien erzielen keine einvernehmliche Lösung über das weitere Vorgehen, steht dem Auftraggeber ein fristloses Sonderkündigungsrecht hinsichtlich der gesamten Auftragsverarbeitung zu. Erfolgt innerhalb von 28 Tagen nach Übersendung der Anzeige kein Einspruch durch den Auftraggeber, gilt die Zustimmung zur Änderung als erteilt.

Nachweispflichten

Subunternehmer - ERFORDERLICH

Göbel+Lenze
Direktmarketing GmbH
Stahlgruberring 22
81829 München

Fon (089) 42 71 88 – 840
fax (089) 42 71 88 – 878
web www.goebel-lenze.de

Deutsche Bank AG
IBAN:
DE65700700240228806600
BIC/SWIFT-CODE:
DEUTDEDBMUC

Geschäftsführer
Wulf Henrichs

Registergericht München HRB 69 740

Finanzamt München
USt.-Id-Nr. DE 129 314 019
Steuernummer 812/45460

Anlage 2

Technische und organisatorische Maßnahmen gemäß Artikel 32 DSGVO

Inhalt

1. Revisionshistorie 14

2. Ziel dieses Dokumentes 14

3. Pseudonymisierung und Verschlüsselung 14

3.1. Pseudonymisierung 14

3.2. Verschlüsselung 14

4. Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit 15

4.1. Vertraulichkeit 15

4.1.1. Zutrittskontrolle 15

4.1.2. Zugangskontrolle 15

4.1.3. Zugriffskontrolle 17

4.1.4. Weitergabekontrolle 18

4.1.5. Trennungskontrolle 19

4.1.6. Löschen von Daten 19

4.2. Integrität 20

4.2.1. Eingabekontrolle 20

4.3. Verfügbarkeit und Belastbarkeit 20

4.3.1. Verfügbarkeitskontrolle 20

4.3.2. Auftragskontrolle 20

5. Wiederherstellung 21

5.1. Verfügbarkeitskontrolle 21

5.2. Notfallplan 21

6. Überprüfung, Bewertung und Evaluierung 22

6.1. Verarbeitung auf Weisung des Auftraggebers 22

6.2. Prüfung der technischen und organisatorischen Maßnahmen 22

6.3. Umgang mit Sicherheitsvorfällen und Störungen 22

6.4. Datenschutzfreundliche Voreinstellungen 22

6.5. Kontrollen von Subdienstleistern 22

7. Kontakt 22

Göbel+Lenze
Direktmarketing GmbH
Stahlgruberring 22
81829 München

Fon (089) 42 71 88 – 840
fax (089) 42 71 88 – 878
web www.goebel-lenze.de

Deutsche Bank AG
IBAN:
DE65700700240228806600
BIC/SWIFT-CODE:
DEUTDEDBMUC

Geschäftsführer
Wulf Henrichs

Registergericht München HRB 69 740

Finanzamt München
USt.-Id-Nr. DE 129 314 019
Steuernummer 812/45460

1. Revisionshistorie

Datum	Änderung	Name
10.04.2018	Erstellung	Wulf Henrichs
18.02.2020	Prüfung und Bestätigung	Wulf Henrichs

2. Ziel dieses Dokumentes

Das vorliegende Dokument beschreibt die technischen und organisatorischen Maßnahmen (TOM) nach Artikel 32 DSGVO bei der Göbel+Lenze Direktmarketing GmbH.
Der Datenschutz besitzt in unserem Unternehmen eine besondere Bedeutung und erfolgt auf der Basis der Datenschutz-Grundverordnung (DSGVO), auf dessen Einhaltung alle in unserem Haus mit der Verarbeitung von personenbezogenen Daten befassten Mitarbeiter schriftlich verpflichtet wurden. Die Durchführung der Verpflichtungen wird während der Laufzeit des Hauptvertrages revisionssicher dokumentiert.
Um einen hohen Datenschutz garantieren zu können, wurden gemäß Artikel 32 DSGVO folgende technische und organisatorische Maßnahmen getroffen und werden laufend gewährleistet:

3. Pseudonymisierung und Verschlüsselung

3.1. Pseudonymisierung

Eine Pseudonymisierung der Kundendaten wird nicht vorgenommen, da die Auftragsdatenverarbeitung explizit die Verwendung und Nutzung der Kundendaten durch den Eindruck der jeweiligen Kundenadresse in den Briefbogen oder auf das Versandkuvert beinhaltet.

3.2. Verschlüsselung

3.2.1 Besteht nach Maßgabe der Auftragsverarbeitung eine Pflicht zur Verschlüsselung, so setzt der Auftragnehmer bei allen Übertragungen und Speicherungen von Auftraggeber-Daten eine Verschlüsselung ein. Dazu können zumindest folgende Verschlüsselungsstandards eingehalten werden: bei symmetrischen Blockchiffren AES mit einer Schlüssellänge von 256 Bit in den Betriebsarten CBC oder CFB.

3.2.2 Darüber hinaus sind die Verschlüsselungsstandards zulässig, die in der Richtlinie „Technische Richtlinie: Kryptographische Verfahren: Empfehlungen und Schlüssellängen, BSI TR-02102“ des Bundesamtes für Sicherheit in der Informationstechnik in der jeweils aktuell gültigen Fassung empfohlen werden.

3.2.3 Sonstige Verfahren müssen im Einzelfall mit dem Auftraggeber abgestimmt und vom Auftraggeber ausdrücklich schriftlich genehmigt werden.

Göbel+Lenze
Direktmarketing GmbH
Stahlgruberring 22
81829 München

Fon (089) 42 71 88 – 840
fax (089) 42 71 88 – 878
web www.goebel-lenze.de

Deutsche Bank AG
IBAN:
DE65700700240228806600
BIC/SWIFT-CODE:
DEUTDEDBMUC

Geschäftsführer
Wulf Henrichs

Registergericht München HRB
69 740

Finanzamt München
USt.-Id-Nr. DE 129 314 019
Steuernummer 812/45460

4. Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit

4.1. Vertraulichkeit

4.1.1. Zutrittskontrolle

Technische bzw. organisatorische Maßnahmen zur Zutrittskontrolle, insbesondere auch zur Legitimation der Berechtigten:
4.1.1.1 Die Räumlichkeiten des Auftragnehmers, in denen Auftraggeber-Daten erhoben, verarbeitet und/oder genutzt werden, dürfen ausschließlich von MitarbeiterInnen und entsprechend dieser Bestimmungen verpflichteten Vertragspartnern des Auftragnehmers genutzt und betreten werden. Ausgenommen hiervon sind Personen, die sich zur Erfüllung der Verpflichtungen aus dieser Vereinbarung in den Räumlichkeiten aufhalten müssen und die dabei während ihres gesamten Aufenthalts von Zutrittsberechtigten im Sinne des Satz 1 dieser Ziffer 4.1.1.1 begleitet werden.

4.1.1.2 Die Eingänge zu den Räumlichkeiten sind mit Sicherheitsschlössern gegen Zutritt Unbefugter gesichert. Der Zugang der Anlieferung zu den Lager- und Produktionsstätten ist videoüberwacht.

4.1.1.3 Türen, Tore und Fenster sind außerhalb der Betriebszeiten fest verschlossen; Türen, Tore und Fenster im Erdgeschoss sowie alle weiteren leicht zu erreichenden Zugänge zu den Räumen sind einbruchhemmend gemäß den Vorgaben der Sicherungsklasse SG1 nach VdS 2333 gesichert. Die Räumlichkeiten sind durch eine Einbruchmeldeanlage mit Anschluss an eine private Notrufzentrale geschützt.

4.1.1.4 Die Vergabe von Zutrittsberechtigungen und von Schlüsseln ist nachvollziehbar dokumentiert. Das Betreten der Räumlichkeiten durch Betriebsfremde wird unverzüglich beim Betreten und für jeweils einen Zeitraum von einem Monat nach Betreten der Räumlichkeiten protokolliert.

4.1.1.5 Die vom Auftragsverarbeiter zur Durchführung von Auftragsverarbeitungen verwendeten Server sind in einem separat abgesicherten Serverraum untergebracht, welche durch eine Zutrittskontrollanlage entsprechend Klasse B nach VdS 2367 gegen den Zutritt Unbefugter gesondert gesichert sind. Diese Räume sind einbruchhemmend geschützt und mindestens gemäß den Vorgaben der Sicherungsklasse SG1 nach VdS 2333 ausgeführt. Der Zutritt zu diesen Räumlichkeiten ist auf das zur Wartung und Instandsetzung sowie auf die im Übrigen konkret erforderlichen Rollen und Personen beschränkt. Unverzüglich beim Betreten und für jeweils einen Zeitraum von 90 Tagen nach Betreten der Räumlichkeiten werden die Zutritte zu diesen Räumlichkeiten protokollieren. Der Auftragsverarbeiter prüft die Protokolle regelmäßig, zumindest stichprobenartig.

4.1.2. Zugangskontrolle

Technische (Kennwort- / Passwortschutz) und organisatorische (Benutzerstammsatz) Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung:
4.1.2.1 Der Auftragnehmer wird die Auftraggeber-Daten bei jeder Übertragung und/oder Speicherung auf mobile Datenträger oder Systeme (insbesondere auf Notebooks und Laptops, Festplatten, CD, DVD, USB-Sticks, Bänder, Speicherkarten) in einer nach dem Stand der Technik geeigneten Form verschlüsseln.

4.1.2.2 Die zur Verarbeitung von Auftraggeber-Daten eingesetzten Systeme des Auftragnehmers sind durch Authentifikations- und Autorisationssysteme geschützt. Dabei verpflichtet

Göbel+Lenze
Direktmarketing GmbH
Stahlgruberring 22
81829 München

Fon (089) 42 71 88 – 840
fax (089) 42 71 88 – 878
web www.goebel-lenze.de

Deutsche Bank AG
IBAN:
DE65700700240228806600
BIC/SWIFT-CODE:
DEUTDEDBMUC

Geschäftsführer
Wulf Henrichs

Registergericht München HRB 69 740

Finanzamt München
USt.-Id-Nr. DE 129 314 019
Steuernummer 812/45460

sich der Auftragnehmer, mindestens Benutzerkennungen und komplexe Passwörter gemäß den Bestimmungen der Ziffer 4.1.2.7 sowie abgestufte Zugriffsrechte gemäß den Bestimmungen der Ziffer 4.1.3 zu verwenden.

4.1.2.3 Der Auftragnehmer verpflichtet sich, die Zugangsberechtigungen zu den zur Verarbeitung der Auftraggeber Daten eingesetzten Systemen (insbesondere in Form von Benutzernamen und Passwörtern) nur an die zur Leistungserbringung eingesetzten MitarbeiterInnen in dem für die jeweilige Aufgabe erforderlichen Umfang zu vergeben. Diese Vergabe von Zugangsberechtigungen wird für die Laufzeit dieses Vertrages in Textform dokumentiert.

4.1.2.4 Alle Zugänge sind personenspezifisch vergeben. Die Benutzung von Kennungen (Accounts) durch mehrere Personen unterbleibt grundsätzlich. Ist in zu begründenden Einzelfällen die Benutzung von Gruppenkennungen unvermeidbar, so ist die Kennung zu jedem Zeitpunkt einer verantwortlichen natürlichen Person zuordenbar.

4.1.2.5 Zu Zwecken der technischen Wartung bestehen gesonderte Zugänge (Accounts), die in der Regel keinen Zugriff auf Auftraggeber-Daten ermöglichen.

4.1.2.6 Bei Verwendung von Passwörtern verpflichtet sich der Auftragnehmer, Passwörter in ausreichender Komplexität und Güte zu wählen. Ausreichende Komplexität und Güte bedeutet dabei mindestens eine Länge von zehn (10) Zeichen bei Nutzung von drei der folgenden 4 Kategorien (Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen), keine Verwendung generischer Begriffe oder von Eigennamen sowie die Unzulässigkeit mindestens der letzten drei (3) verwendeten Passwörter

4.1.2.7 Passwörter werden durch den Besitzer der zugehörigen Kennung persönlich vergeben und spätestens alle dreißig (30) Tage durch diesen geändert. Dieser Vorgang wird technisch oder organisatorisch erzwungen und nachhaltig für eine Mindestdauer von einem Jahr dokumentiert. Bei mehr als fünf (5) Fehleingaben eines Passwortes in Folge ist der Zugang gesperrt und wird nur nach einer erneuten Prüfung der Zugangsberechtigung wieder freigegeben.

4.1.2.8 Authentifikationsdaten (insbesondere Passwörter und kryptographische Schlüssel) werden streng geheim gehalten und gegenüber unbefugten Dritten nicht bekannt gegeben. Der Auftragnehmer stellt sicher, dass diese Authentifikationsdaten nicht im Klartext aufbewahrt und diese ausschließlich unter Einsatz einer Ziffer 4.1.7 entsprechenden Verschlüsselung oder als unumkehrbare kryptographische Prüfsumme verarbeitet und genutzt (insbesondere gespeichert und übertragen) werden. Sofern Unbefugte Kenntnis von Zugangsdaten erhalten, zeigt der Auftragsverarbeiter dies unverzüglich beim Auftragnehmer an.

4.1.2.9 Sofern Authentifikationsdaten im begründeten Einzelfall aus technischen oder organisatorischen Gründen nicht verschlüsselt übertragen werden können (z.B. für Initialpassworte oder Passwort-Zurücksetzungen), finden Einweg-Passwörter Verwendung. Hierbei ist technisch sichergestellt, dass die übermittelten Passwörter unmittelbar nach der Verwendung geändert werden müssen. Der Auftragnehmer stellt weiterhin sicher, dass die Authentifikationsdaten ausschließlich an zuvor authentifizierte berechtigte Empfänger übermittelt werden.

4.1.2.10 Soweit das Betriebssystem oder die eingesetzte Software die Möglichkeit bietet, Formulareingaben und/oder Passwörter zu speichern, verpflichtet sich der Auftragnehmer, diese Funktionalität in Bezug auf die Daten des Auftraggebers zu deaktivieren.

Göbel+Lenze
Direktmarketing GmbH
Stahlgruberring 22
81829 München

Fon (089) 42 71 88 – 840
fax (089) 42 71 88 – 878
web www.goebel-lenze.de

Deutsche Bank AG
IBAN:
DE65700700240228806600
BIC/SWIFT-CODE:
DEUTDEDBMUC

Geschäftsführer
Wulf Henrichs

Registergericht München HRB
69 740

Finanzamt München
USt.-Id-Nr. DE 129 314 019
Steuernummer 812/45460

4.1.2.11 Der Auftragnehmer stellt sicher, dass Netze mit unterschiedlichen Verwendungszwecken und/oder Sicherheitsniveaus durch Firewalls getrennt, sowie diese Firewalls unverzüglich an neue technische Entwicklungen angepasst werden. Insbesondere wird sichergestellt, dass jede Firewall zumindest eine zustandsgesteuerte und regelbasierte Paketfilterung umsetzt und dass der zur Anwendung kommende Regelsatz die Kommunikation von und zu den Systemen, mit welchen Auftraggeber-Daten erhoben, verarbeitet und/oder genutzt werden, mittels expliziter Freigaben ("Whitelist") auf die minimal für den Betrieb dieser Systeme notwendigen Verbindungen einschränkt. Sämtliche nachträgliche Änderungen an der Konfiguration der Firewall und/oder dem zur Anwendung kommenden Regelsatz werden unter strikter Beachtung einer Rollentrennung ("4-Augen-Prinzip") vorab genehmigt und während der Dauer des Vertrages dauerhaft und nachvollziehbar ("revisionssicher") dokumentiert.

4.1.2.12 Der Auftragnehmer verpflichtet sich, auf allen zur Verarbeitung von Auftraggeber-Daten eingesetzten Systemen speicherresidente Virenscanner mit mindestens täglichen Updates sowie eine Personal Firewall einzusetzen. Der Auftragnehmer unterlässt es, Systeme, die zur Verarbeitung von Auftraggeber-Daten eingesetzt werden, direkt d.h. ohne mindestens Einsatz der Sicherheitsmaßnahmen gemäß Satz 1 dieser Ziffer 4.1.2.12. an das Internet anzubinden.

4.1.2.13 Originaldokumente oder Datenträger werden zur lückenlosen Verwaltung beim Empfang eindeutig gekennzeichnet (bei Originaldokumenten durch Paginierung, bei Datenträgern durch eine fortlaufende Nummerierung).

4.1.3. Zugriffskontrolle

Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung:
4.1.3.1 Der Auftragnehmer hat für sämtliche Zugriffe auf Auftraggeber-Daten ein abgestuftes und geeignetes granulares Rechtesystem eingerichtet und technisch dauerhaft implementiert. Die Zugriffsrechte sind so gestaltet, dass sie nur den für die Leistungserbringung eingesetzten MitarbeiterInnen jeweils im für die Erfüllung der konkreten Aufgaben notwendigen Umfang Zugriff auf die Auftraggeber-Daten erlauben. Die Rechte wurden dabei durch eine auf das zwingend erforderliche Maß begrenzte Anzahl an MitarbeiterInnen des Auftragnehmers mit Administratorenrechten vergeben und verwaltet. Diese Rechtevergabe wird für die Laufzeit dieses Vertrages in Textform dokumentiert.

4.1.3.2 Bei den zur Verarbeitung von Auftraggeber-Daten eingesetzten Systemen des Auftragnehmers sind Bildschirme oder andere Ausgabegeräte so angeordnet, dass unbeteiligte MitarbeiterInnen und sonstige Dritte keinen Einblick in Auftraggeber-Daten nehmen können.

4.1.3.3 Bei allen zur Verarbeitung von Auftraggeber-Daten eingesetzten Systemen ist sichergestellt, dass eine Nutzung von Kennungen nicht durch andere Personen als den berechtigen Nutzer möglich ist. Arbeitsstationen, die einen Zugriff auf Auftraggeber-Daten ermöglichen, sind bei jedem Verlassen der Systeme durch einen passwortgeschützten Bildschirmschoner vor unberechtigten Zugriffen geschützt. Dieser Bildschirmschoner aktiviert sich zudem bei Inaktivität des angemeldeten Benutzers spätestens nach fünf (5) Minuten automatisch.

4.1.3.4 Nach Ziffer 4.1.2.13 gekennzeichnete Originaldokumente oder Datenträger werden durch die den Prozess verantwortlich leitenden MitarbeiterInnen an die mit der

Göbel+Lenze
Direktmarketing GmbH
Stahlgruberring 22
81829 München

Fon (089) 42 71 88 – 840
fax (089) 42 71 88 – 878
web www.goebel-lenze.de

Deutsche Bank AG
IBAN:
DE65700700240228806600
BIC/SWIFT-CODE:
DEUTDEDBMUC

Geschäftsführer
Wulf Henrichs

Registergericht München HRB 69 740

Finanzamt München
USt.-Id-Nr. DE 129 314 019
Steuernummer 812/45460

Leistungserbringung beauftragten MitarbeiterInnen herausgegeben und von diesen nach Abschluss der Arbeit wieder entgegengenommen. Diese Dokumente und Datenträger werden in ordnungsgemäß verschlossenen, und ausschließlich für die Durchführung dieser Auftragsverarbeitung genutzten Datensicherungsschränken verwahrt, wenn und solange sie nicht in der Bearbeitung sind.

4.1.3.5 Originaldokumente, Datenträger und jegliche Auftraggeber-Daten in Papierform sind auch während der Bearbeitung vor unberechtigtem Zugriff geschützt. BearbeiterInnen sind angewiesen diese bei jedem - auch nur kurzzeitigem - Verlassen des Arbeitsplatzes vor unberechtigtem Zugriff zu schützen ("Clean Desk Policy").

4.1.3.6 Soweit Abbilder von Originaldokumenten mit Auftraggeber-Daten in elektronischer Form erfasst und abgelegt werden, sind die resultierenden Bilddateien in verschlüsselter Form nach Maßgabe der Ziffer 4.1.10 gespeichert. Der Zugriff auf diese Dokumente ist durch Zugriffsrechte gemäß Ziffer 4.1.3.1 beschränkt, insbesondere sind Zugriffe von Administratoren und nicht mit der direkten Leistungserbringung befassten Personen auf die Inhalte nicht zulässig.

4.1.4. Weitergabekontrolle

Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung:
4.1.4.1 Der Auftragnehmer stellt sicher, dass Auftraggeber-Daten nicht unbefugt kopiert (insbesondere auf externe Datenträger gespeichert) weitergegeben und/oder gelöscht werden können.

4.1.4.2 Die Verwendung externer Speichermedien (insbesondere USB-Sticks, externe Festplatten, SD-Karten, CD und DVD-Brenner) ist durch technische Maßnahmen wie beispielsweise den Einsatz einer Software zur Schnittstellenkontrolle oder eine vollständige Deaktivierung der die Übertragung der Auftraggeber-Daten ermöglichenden Geräte und Schnittstellen (insbesondere USB-Ports, Card Reader, PCMCIA, IEEE1394, Bluetooth sowie WLAN) dahingehend eingeschränkt, dass Auftraggeber-Daten nicht über den zur Vertragserfüllung erforderlichen Umfang hinaus kopiert und/oder weitergegeben werden können. Die Maßnahmen werden durch den Auftragnehmer in ihrer Wirksamkeit durch stichprobenartige Kontrollen regelmäßig überprüft.

4.1.4.3 Soweit den zur Verarbeitung von Auftraggeber-Daten eingesetzten MitarbeiterInnen der Zugang zu Email und Internet ermöglicht ist, ist durch geeignete Kontroll- und Filtermaßnahmen wie beispielsweise den Einsatz eines restriktiv konfigurierten URL-Filters, Filterung von E-Mail Anhängen und/oder eine stichprobenartige Auswertung des Mailverkehrs verhindert, dass Auftraggeber-Daten unbefugt über das Internet weitergegeben werden.

4.1.4.4 Die mit der Verarbeitung von Auftraggeber-Daten befassten MitarbeiterInnen verfügen nicht über Administratorenrechte für die zur Verarbeitung von Auftraggeber-Daten eingesetzten Systeme. Davon ausgenommen sind die Geschäftsführer des Auftragnehmers.

4.1.4.5 Der Auftragnehmer stellt sicher, dass auf Systemen, mit denen Auftraggeber-Daten verarbeitet werden, keine Software eingesetzt wird, bei der nicht durch eine aktive Kontrollmöglichkeit durch den Auftragnehmer ausgeschlossen ist, dass diese Software Auftraggeber-Daten an Dritte übermittelt.

Göbel+Lenze
Direktmarketing GmbH
Stahlgruberring 22
81829 München

Fon (089) 42 71 88 – 840
fax (089) 42 71 88 – 878
web www.goebel-lenze.de

Deutsche Bank AG
IBAN:
DE65700700240228806600
BIC/SWIFT-CODE:
DEUTDEDBMUC

Geschäftsführer
Wulf Henrichs

Registergericht München HRB 69 740

Finanzamt München
USt.-Id-Nr. DE 129 314 019
Steuernummer 812/45460

4.1.4.6 Die Nutzung von über das Internet angebotenen Diensten Dritter zur Verarbeitung von Auftraggeber-Daten, wie beispielsweise Übersetzungsdienste, wird vom Auftragnehmer unterlassen.

4.1.4.7 In den Räumlichkeiten des Auftragnehmers, in denen Auftraggeber-Daten verarbeitet werden, ist der Zugang zu technischen Einrichtungen, die zur Anfertigung von Kopien geeignet sind (insbesondere Fotokopierer) sowie zu Druckern, durch ein abgestuftes Zugriffskonzept und/oder Zugangscodes sichergestellt, dass der Zugriff auf diese Geräte nur durch besonders instruierte MitarbeiterInnen (z.B. Projekt- oder TeamleiterInnen, Führungskräfte) im zu deren Aufgabenerfüllung notwendigen Umfang möglich ist.

4.1.4.8 Bei jenen Systemen des Auftragnehmers mit nicht-flüchtigem Speicher (beispielsweise Netzwerkdrucker oder Scanner), ist durch den Auftragnehmer sichergestellt, dass durch diese Systeme keine Auftraggeber-Daten über den unmittelbar zur Vertragsdurchführung erforderlichen Umfang hinaus gespeichert werden. Der Auftragnehmer stellt durch technische Maßnahmen sicher, dass Dritte (insbesondere ggf. zur Wartung der Systeme eingesetzte externe Dienstleister) nicht auf Auftraggeber-Daten zugreifen können.

4.1.5. Trennungskontrolle

Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken:
Der Auftragnehmer kommt der Verpflichtung nach, die Auftraggeber-Daten so zu verarbeiten, dass eine vollständige Trennung der Auftraggeber-Daten von Daten anderer Auftraggeber oder Eigendaten des Auftragnehmers gemäß den vergebenen Zugriffsrechten gemäß Ziffer 4.1.3.1 (mindestens aber auf Ebene der zur Verarbeitung eingesetzten Anwendungen) gewährleistet ist.
Insbesondere ist sichergestellt, dass die Auftraggeber-Daten jederzeit vollständig identifiziert und auch vollständig gelöscht werden können. Auftraggeber-Daten, die zu unterschiedlichen Zwecken verarbeitet werden, sind ebenfalls nach dieser Maßgabe getrennt voneinander zu verarbeiten.

4.1.6. Löschen von Daten

4.1.6.1 Der Auftragnehmer stellt sicher, dass sämtliche löschbaren elektronischen Datenträger (insbesondere Festplatten, USB-Sticks, Bänder), die Auftraggeber-Daten enthalten, datenschutzgerecht und nicht wieder herstellbar gelöscht werden können. Ist aufgrund eines Defekts oder aufgrund der Eigenheiten des Datenträgers eine derartige Löschung nicht möglich, so wird der Datenträger entsprechend Ziffer 4.1.6.2 vernichtet.

4.1.6.2 Der Auftragnehmer wird sämtliche Papierdokumente und alle nicht-löschbaren Datenträger (einschließlich sämtlicher Fehldrucke bzw. Fehlspeicherungen, sowie CDs und DVDs), die Auftraggeber-Daten enthalten, mit einem handelsüblichen Dokumentenvernichter gemäß der Sicherheitsstufe 4 , Schutzklasse 2 nach DIN-Norm 66399 oder einem mindestens gleichwertigen Verfahren vernichten.

4.1.6.3 Auftraggeber-Daten in Datenbanksystemen werden so aus der logischen Struktur gelöscht, dass zuverlässig sichergestellt ist, dass die Löschung weder rückgängig gemacht noch anderweitig auf die gelöschten Daten zugegriffen werden kann.

4.1.6.4 Die Löschung wird für die Dauer der Laufzeit des Hauptvertrags mit dem Auftraggeber protokolliert.

Göbel+Lenze
Direktmarketing GmbH
Stahlgruberring 22
81829 München

Fon (089) 42 71 88 – 840
fax (089) 42 71 88 – 878
web www.goebel-lenze.de

Deutsche Bank AG
IBAN:
DE65700700240228806600
BIC/SWIFT-CODE:
DEUTDEDBMUC

Geschäftsführer
Wulf Henrichs

Registergericht München HRB 69 740

Finanzamt München
USt.-Id-Nr. DE 129 314 019
Steuernummer 812/45460

4.2. Integrität

4.2.1. Eingabekontrolle

Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind:
Der Auftragnehmer stellt eine bis zur Löschung der Auftraggeber-Daten dauerhafte Protokollierung und organisatorische Maßnahmen sicher, dass auf Verlangen des Auftraggebers jederzeit, auch nachträglich, zuverlässig festgestellt werden kann ob, wann, wo und von wem Auftraggeber-Daten erhoben, verarbeitet und/oder genutzt wurden (wenigstens durch eine Protokollierung der Benutzerkennung des/der zugreifenden Mitarbeiters/in, des geänderten Datums und des Zeitpunktes der Änderung in den Logfiles der jeweiligen Systeme für mindestens 90 Tagen).

4.3. Verfügbarkeit und Belastbarkeit

4.3.1. Verfügbarkeitskontrolle

Maßnahmen zur Datensicherung (physikalisch / logisch):
4.3.1.1 Der Auftragnehmer schützt die Auftraggeber-Daten durch technische und organisatorische Maßnahmen vor Verlust durch zufällige, fahrlässige oder vorsätzliche Löschung oder Veränderung.

4.3.1.2 Der Auftragnehmer fertigt in regelmäßigen Abständen - mindestens einmal täglich - Sicherungskopien der Auftraggeber-Daten an und bewahrt diese in einem Datensicherungsschrank der Güteklasse S 60 DIS auf. Die Wiedererstellbarkeit der gesicherten Daten wird stichprobenartig geprüft; die Überprüfung wird fortlaufend dokumentiert.

4.3.1.3 Der Auftragnehmer stellt sicher, dass sämtliche Software auf Systemen, die zur Verarbeitung von Auftraggeber-Daten eingesetzt werden, aktuell gehalten sowie sicherheitsrelevante Aktualisierungen (Updates, Patches, Fixes) unverzüglich eingespielt werden, nachdem diese vom Hersteller der Software allgemein verfügbar gemacht wurden. Bei als „kritisch“ oder sinngemäß qualifizierten Updates beträgt die Frist nach Satz 1 dieser Ziffer

4.3.1.3 höchstens zwei (2) Werktage.

4.3.1.4 Der Auftragnehmer stellt sicher, dass die Server-Systeme gegen Ausfall und Datenverlust abgesichert sind. Hierbei werden RAID-Systeme eingesetzt, in denen über gespiegelte Festplatten ein Datenverlust ausgeschlossen wird. Die Serversysteme sind mit USV-Anlagen abgesichert, um kurzfristige Stromausfälle zu covern bzw. ab einem Stromausfall von 30 Minuten die Systeme gesichert herunterzufahren. Zur Brandabsicherung ist der Serverraum mit einem Brandmelder ausgestattet, der auf einen Fernüberwachungsdienst aufgeschaltet ist, um im Schadenfall die Feuerwehr zu verständigen.

4.3.2. Auftragskontrolle

Maßnahmen (technisch / organisatorisch) zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer:
4.3.2.1 Ohne explizite Weisung des Auftraggebers findet keine Auftragsverarbeitung statt. Die Weisung des Auftraggebers erfolgt schriftlich oder in elektronischer Form. Sollte die Weisung mündlich erfolgen, wird diese vom Auftraggeber schriftlich im Nachhinein bestätigt oder vom Auftragnehmer schriftlich zurückbestätigt.

Göbel+Lenze
Direktmarketing GmbH
Stahlgruberring 22
81829 München

Fon (089) 42 71 88 – 840
fax (089) 42 71 88 – 878
web www.goebel-lenze.de

Deutsche Bank AG
IBAN:
DE65700700240228806600
BIC/SWIFT-CODE:
DEUTDEDBMUC

Geschäftsführer
Wulf Henrichs

Registergericht München HRB 69 740

Finanzamt München
USt.-Id-Nr. DE 129 314 019
Steuernummer 812/45460

4.3.2.2 Unterauftragnehmer, die mit einer Auftragsverarbeitung Im Sinne von Art. 28 DSGVO beauftragt werden, werden nur mit Einwilligung des Auftraggebers eingesetzt. Hierbei wird mit dem Unterauftraggeber eine analoge Datenschutzvereinbarung nach Art. 28 DSGVO geschlossen.

4.3.2.3 Über die allgemeinen Grundsätze sowie über die sich aus einer Auftragsverarbeitung ergebenden spezifischen Anforderungen des Datenschutzes, einschließlich der Datensicherheit, werden die beim Auftragsverarbeiter zur Durchführung dieser Auftragsverarbeitung beschäftigten Personen vor dem Einsatz beim Auftragsverarbeiter zur Durchführung dieser Auftragsverarbeitung und sodann regelmäßig umfassend geschult. Die Durchführung der Schulungen wird während der Laufzeit des Hauptvertrages revisionssicher dokumentiert.

4.3.2.4 Zum Ende eines jeden Quartals wird ein Bericht über die im abgelaufenen Quartal beim Auftragsverarbeiter zur Durchführung dieser Auftragsverarbeitung beschäftigten und nach Maßgabe der in Ziffer 4.3.2.3 geschulten und nach Ziffer 2 verpflichteten Personen erstellt. Dieser Bericht wird dem Auftraggeber nach Erstellung unverzüglich übergeben.

5. Wiederherstellung

5.1. Verfügbarkeitskontrolle

Maßnahmen zur Datensicherung (physikalisch / logisch):
5.1.1 Der Auftragnehmer fertigt in regelmäßigen Abständen - mindestens einmal täglich - Sicherungskopien der Auftraggeber-Daten an und bewahrt diese in einem Datensicherungsschrank der Güteklasse S 60 DIS auf. Die Wiedererstellbarkeit der gesicherten Daten wird stichprobenartig geprüft; die Überprüfung wird fortlaufend dokumentiert.

5.1.2 Der Auftragnehmer stellt sicher, dass sämtliche Software auf Systemen, die zur Verarbeitung von Auftraggeber-Daten eingesetzt werden, aktuell gehalten sowie sicherheitsrelevante Aktualisierungen (Updates, Patches, Fixes) unverzüglich eingespielt werden, nachdem diese vom Hersteller der Software allgemein verfügbar gemacht wurden und vom Auftragsverarbeiter im Rahmen eines dem Stand der Technik entsprechenden Verfahren getestet werden. Bei als „kritisch“ oder sinngemäß qualifizierten Updates beträgt die Frist nach Satz 1 dieser Ziffer 4.3.1.3 höchstens zwei (2) Werktage.

5.1.3 Der Auftragnehmer stellt sicher, dass die Server-Systeme gegen Ausfall und Datenverlust abgesichert sind. Hierbei werden RAID-Systeme eingesetzt, in denen über gespiegelte Festplatten ein Datenverlust ausgeschlossen wird. Die Serversysteme sind mit USV-Anlagen abgesichert, um kurzfristige Stromausfälle zu covern bzw. ab einem Stromausfall von 30 Minuten die Systeme gesichert herunterzufahren. Zur Brandabsicherung ist der Serverraum mit einem Brandmelder ausgestattet, der auf einen Fernüberwachungsdienst aufgeschaltet ist, um im Schadenfall die Feuerwehr zu verständigen.

5.2. Notfallplan

Der Auftragnehmer verfügt über ein umfangreiches Notfallkonzept, in dem dokumentiert ist wie sich die Mitarbeiter des Auftragnehmers im Notfall zu verhalten haben, welcher Mitarbeiter des Auftragnehmers welche Verantwortung trägt und wie sowohl die IT-Systeme als auch Druck- und Produktionssysteme wiederbeschafft, installiert und in Betrieb genommen werden, um das Unternehmen ohne Datenverluste wieder in Gang zu setzen.

Göbel+Lenze
Direktmarketing GmbH
Stahlgruberring 22
81829 München

Fon (089) 42 71 88 – 840
fax (089) 42 71 88 – 878
web www.goebel-lenze.de

Deutsche Bank AG
IBAN:
DE65700700240228806600
BIC/SWIFT-CODE:
DEUTDEDBMUC

Geschäftsführer
Wulf Henrichs

Registergericht München HRB 69 740

Finanzamt München
USt.-Id-Nr. DE 129 314 019
Steuernummer 812/45460

6. Überprüfung, Bewertung und Evaluierung

6.1. Verarbeitung auf Weisung des Auftraggebers

Um zu gewährleisten, dass die Auftragsverarbeitung personenbezogener Daten, deren Bearbeitung über die reine Adressierung mit oder ohne Anrede hinausgeht, nur entsprechend den Weisungen des Auftraggebers erfolgt, wird bei Aufträgen, für die keine detaillierte schriftliche Weisung des Auftraggebers bezüglich der Verwendung weiterer personenbezogener Merkmale vorliegt, die vorgesehene Verarbeitung dieser Daten vom Auftragnehmer in einer Auftragsbestätigung oder sonstigen schriftlichen Mitteilung an den Auftraggeber bestätigt.

6.2. Prüfung der technischen und organisatorischen Maßnahmen

Die Wirksamkeit der technischen und organisatorischen Maßnahmen wird intern sowie u.a. durch den Externen Datenschutzbeauftragten laufend überprüft, bewertet und evaluiert.

6.3. Umgang mit Sicherheitsvorfällen und Störungen

Der Auftragnehmer hat einen Prozess für den Umgang mit Sicherheitsvorfällen festgelegt. Dieser ist jedem Mitarbeiter bekannt. Aufgetretene Sicherheitsverletzungen und Systemstörungen werden, je nach Art, nach Bekanntwerden mit Beratung des Datenschutzbeauftragten und/oder des IT-Verantwortlichen bewertet und auch entsprechend dokumentiert.

6.4. Datenschutzfreundliche Voreinstellungen

Im konkreten Bezug zur auftragsgegenständlichen Verarbeitung ist die Art und Weise der Verarbeitung vom Auftraggeber vorgeschrieben. Wo immer möglich wird jedoch der Umfang der personenbezogenen Daten auf das mindeste begrenzt.

6.5. Kontrollen von Subdienstleistern

Die Subdienstleister der Göbel+Lenze Direktmarketing GmbH werden regelmäßig geprüft.

7. Kontakt

Göbel+Lenze Direktmarketing GmbH
Stahlgruberring 22
81829 München
Geschäftsführer: Wulf Henrichs
Telefon: +49 89 427188-840
Telefax: +49 89 427188-872

Göbel+Lenze
Direktmarketing GmbH
Stahlgruberring 22
81829 München

Fon (089) 42 71 88 – 840
fax (089) 42 71 88 – 878
web www.goebel-lenze.de

Deutsche Bank AG
IBAN:
DE65700700240228806600
BIC/SWIFT-CODE:
DEUTDEDBMUC

Geschäftsführer
Wulf Henrichs

Registergericht München HRB
69 740

Finanzamt München
USt.-Id-Nr. DE 129 314 019
Steuernummer 812/45460